

(use as many sheets as necessary)

Sheet	1	of	1
-------	---	----	---

Sheet	1	of	1
-------	---	----	---

Application Number	10/523840
--------------------	-----------

Filing Date	February 8, 2005
--------------------	------------------

First Named Inventor	Olivier Billet et al.
-----------------------------	-----------------------

Examiner Name	Smithers
---------------	----------

Attorney Docket Number	032326-293
------------------------	------------

Examine
Initials

Document
NumberKind Code
(if known)Name of Patentee or Applicant
of Cited Document

Issue/Publication Date
(MM-DD-YYYY)

Examiner

Document

Kind Code

Country

Date of Publication
(MM-DD-YYYY)

STATUS

Translation

Translation

Partial

Eng. Lang

Report

Course

input

Abstract

Examiner
Initials

Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.

/MBS/ CHUDNOVSKY D.V. et al., "Sequences of Numbers Generated By Addition In Formal Groups and New Primality and Factorization Tests", Advances in Applied Mathematics, Academic Press, Vol. 7, 1986, pages 385-434.

/MBS/ BRIER E. et al., "Weierstrass Elliptic Curves and Side-Channel Attacks", 5th International Workshop on Practice and Theory in Public Key Cryptosystems, February 2002, pages 335-345.

/MBS/ JOYE M. et al., "Hessian Elliptic Curves and Side-Channel Attacks", Cryptographic Hardware and Embedded Systems Ches. Third International Workshop, Vol. 2162, May 14, 2001, pages 402-410.

/MBS/ KHELDOUNI A. et al., "Elliptic Cohomology Operation Defined By Hecke Operator T2", Vol. 324, No. 2, January 1997, pages 215-220.

/MBS/ P. BARRETO et al., "Constructing Elliptic Curves With Prescribed Embedding Degrees", Security in Communication Networks, Third International Conference, September 2002, pages 257-267.

Examiner Signature	/Matthew B Smithers/
-----------------------	----------------------

Date
Considered

04/16/2009

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with M.P.E.P. § 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to Applicant.